UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

NATALIE STEVENSON, on behalf of herself individually and on behalf of all others similarly situated, Plaintiff, v. PAYCHEX INC., Defendant.	**CASE NO. 24-6433** **CLASS ACTION COMPLAINT** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiff NATALIE STEVENSON ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant PAYCHEX INC., ("Paychex" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. The Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of consumers' highly personal information, including names and Social Security numbers ("personal identifying information" or "PII").

3. Paychex's breach differs from typical data breaches because it affects consumers who had no relationship with Paychex, never sought one, and never consented to Paychex collecting and storing their information.

4. On information and belief, the Data Breach occurred on April 30, 2024, when Paychex attempted to exchange information with the State of California regarding unclaimed property but instead allowed an unauthorized individual access to the information instead.

5. On or about May 22, 2024–almost a month after the Data Breach occurred–Paychex finally began notifying Class Members about the Data Breach ("Breach Notice"). A sample Breach Notice is attached as Exhibit A. However, upon information and belief, Paychex has not completed notifying all affected victims of the breach, with Plaintiff still awaiting a breach notice as of July 2024, almost three months after the Data Breach first occurred.

6. Paychex waited at least a month after the discovery of the Data Breach before informing Class Members about the Data Breach, even though Plaintiff and thousands of Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

7. Paychex's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its consumers how many people were impacted, how the breach happened on Paychex's systems, or why it took Paychex a month to begin notifying victims that hackers had gained access to highly private PII.

8. Defendant's failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

10. In failing to adequately protect Plaintiff's and the Class's PII, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former consumers.

11. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiff is a Data Breach victim.

13. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

14. Plaintiff, Natalie Stevenson, is a natural person and citizen of Florida, where she intends to remain.

15. Defendant, Paychex, is a New York and Delaware company, incorporated in Delaware with its principal place of business at 911 Panorama Trail South, Rochester, NY 14625.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of

$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. Plaintiff and Defendant are citizens of different states.

17. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

18. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

Paychex

19. Paychex boasts that it "lead[s] the way by making complex HR, payroll, and benefits brilliantly simple." Paychex further claims it is "a leading provider of integrated human capital management solutions for payroll, benefits, human resources, and insurance services"[1] for "approximately 740,000 customers[.]"[2] Paychex boasts a total annual revenue of $5.2 billion.[3]

20. Paychex's HR services are specialized for corporations and employers who oversee highly sensitive data. Paychex thus must oversee, manage, and protect the PII of its clients' customers, Paychex's consumers.

21. On information and belief, these third-party consumers, whose PII was collected by Paychex, do not directly do any business with Paychex.

22. As a self-proclaimed leader in its industry handling highly sensitive aspects of its clients' business, Paychex understood the need to protect its client's customers' data and prioritize its data security.

[1] LinkedIn, Paychex, https://www.linkedin.com/company/paychex/ (last visited July 7, 2024).
[2] Paychex, https://www.paychex.com/ (last visited July 7, 2024).
[3] Paychex, Zoominfo, https://www.zoominfo.com/c/paychex-inc/29803080 (last visited July 7, 2024).

23. Indeed, Paychex makes a multitude of promises in its privacy policy, including that it utilizes "reasonable care to protect the confidentiality, integrity, and availability of Your information and we continue to invest in our award-winning security capabilities..."[4]

> Paychex uses reasonable care to protect the confidentiality, integrity, and availability of Your information and we continue to invest in our award-winning security capabilities, including personnel security and physical security; system security, access control, and monitoring; data backup and business continuity management; and vulnerability and intrusion detection. Specifically, we:
>
> - Maintain policies and procedures covering physical and logical access to our workplaces, systems, and records
> - Apply physical, electronic, and procedural safeguards aligned with industry-recognized best practices
> - Use technology such as backups, virus detection and prevention, firewalls, and other computer hardware and software to protect against unauthorized access to or alteration of Your information
> - Encrypt sensitive information transmitted over the internet
> - Through formal approval processes, access controls, and internal auditing, limit our employee's access to Client information to those who have a business reason to know
> - Require our employees to take information security awareness training upon hire and annually thereafter and apply this training to their jobs every day
> - Provide ongoing training and awareness to our employees about security best practices, including internal phishing simulations for education and testing purposes
> - Use advanced technologies for the backup and recovery of Your information
> - Monitor compliance with established policies through ongoing security risk assessments and internal audits

24. Paychex further claims that "at Paychex, the safety and security of your personal and account information are among our top priorities [,]" further boasting it had an "industry-leading A rating by Security Scorecard."[5]

[4] Privacy Policy, Paychex, https://www.paychex.com/corporate/security/privacy#ccpacookies (last visited July 7, 2024).
[5] Paychex, Privacy & Security, https://www.paychex.com/corporate/security (last visited July 7, 2024).

25. Indeed, so confident was Paychex about its cybersecurity abilities and cybersecurity knowledge, that it regularly released blog posts regarding a variety of cybersecurity information and advice, including "Trickbox using fake Paychex email domain to deliver malware" and "[b]eware of phishing campaign targeting W-2 information."[6]

26. Despite recognizing its duty to do so, on information and belief, Paychex has not implemented reasonably cybersecurity safeguards or policies to protect its consumers' PII or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Paychex leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

The Data Breach

27. Plaintiff is unsure how Paychex got her information but assumes her employer, Emerald Hills Dental Center, which uses Paychex for payroll services, provided Paychex with her PII.

28. On information and belief, Defendant collects and maintains consumers' PII in its computer systems.

29. In collecting and maintaining PII, Defendant implicitly agrees that it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

30. According to its Breach Notice, in "on April 30, 2024", Paychex discovered that, while in the process of exchanging information with the State of California, it had inadvertently exposed its consumers' PII to an unauthorized third party. Ex. A.

[6] *Id.*

31. In other words, Paychex's investigation revealed that Defendant's cyber and data security systems were completely inadequate that it not only allowed, but actually provided, an unauthorized individual, likely a cybercriminal, files containing a treasure trove of thousands of its consumers' highly private PII.

32. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

33. On or around March 22, 2024 –approximately a month after the Breach first began occurring – Paychex finally notified some of its consumers and clients about the Data Breach. Upon information and belief, as of July 2024, Paychex's notification is ongoing, with some consumers, including Plaintiff, not yet being notified of this Data Breach.

34. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing consumers' PII, as evidenced by the Data Breach.

35. Typically, in response to a Data Breach, companies will make assurances and set forth steps in its Breach Notice on how it plans to improve its cybersecurity systems in order to prevent similar breaches in the future. Not Defendant.

36. Despite recognizing the actual imminent harm and injury that flowed from the Data Breach, Defendant here places the onus on Plaintiff, warning victims to "remain vigilant by regularly reviewing your account statements and credit reports closely[,]" and advising that if "you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained [as well as] promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC)." Ex. A.

37. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

38. On information and belief, Paychex offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

39. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

40. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they suffered and will suffer.

41. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

42. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the HR industry preceding the date of the breach.

43. In light of recent high profile data breaches at other financial partner and provider companies, Defendant knew or should have known that its electronic records and consumers' PII would be targeted by cybercriminals.

44. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[7] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[8]

45. Indeed, cyberattacks against the financial industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[9]

46. Cyberattacks on financial systems and banking partner and provider companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a

[7] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 5, 2023).
[8] *Id*.
[9] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited March 13, 2023).

warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[10]

47. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Paychex.

Plaintiff's Experience

48. Plaintiff' employer utilizes Paychex for HR and payroll services and is a Data Breach victim. Plaintiff is still awaiting a formal letter from Paychex regarding which of her PII was exposed by Paychex in the Data Breach.

49. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it.

50. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

51. Plaintiff does not recall ever learning that her PII was compromised in a data breach incident, other than the breach at issue in this case.

52. Plaintiff suffered actual injury from the exposure of her PII —which violates her rights to privacy.

53. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the impacts of the Data Breach, self-monitoring ger accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

[10] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 13, 2023).

54. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

55. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

56. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

57. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

58. Indeed, following the Data Breach, the personal and highly private information on Plaintiff's Paychex account, which Plaintiff's employer utilizes for payroll, was changed without her knowledge or authorization, suggesting her PII is now in the hands of cybercriminals. Upon information and belief, Plaintiff's private information was changed on her Paychex account by cybercriminals in an attempt to deposit Plaintiff's paychecks as their own.

59. Further, shortly after the Data Breach, Plaintiff has suffered a significant increase in spam emails, further suggesting that her PII is now in the hands of cybercriminals.

60. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised

to gather and steal even more information.[11] On information and belief, Plaintiff's Paychex account login and email information was compromised as a result of the Data Breach.

61. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

62. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

63. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent

[11] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

64. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

65. The value of Plaintiff's and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

66. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

67. One such example of criminals using PII for profit is the development of "Fullz" packages.

68. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

69. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

70. Defendant disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

71. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

72. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued

numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

73. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

74. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

75. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

76. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

77. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

78. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

79. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

80. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

81. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

82. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

83. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach including all those who received notice of the breach.

84. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

85. Plaintiff reserves the right to amend the class definition.

86. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of several thousand members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

   i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

   ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

   iii. Whether Defendant were negligent in maintaining, protecting, and securing PII;

   iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

   v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

   vi. Whether Defendant's Breach Notice was reasonable;

   vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

87. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Classes)

88. Plaintiff realleges all previous paragraphs as if fully set forth below.

89. Plaintiff and members of the Classes entrusted their PII to Defendant. Defendant owed to Plaintiff and other members of the Classes a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

90. Defendant owed a duty of care to Plaintiff and members of the Classes because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Classes' PII by disclosing and providing access to this information to third parties and by

failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

91. Defendant owed to Plaintiff and members of the Classes a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Classes the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Classes to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

92. Defendant owed these duties to Plaintiff and members of the Classes because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Classes' personal information and PII.

93. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

94. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff's and members of the Classes' and the importance of exercising reasonable care in handling it.

95. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the

personal information and PII of Plaintiff and members of the Classes which actually and proximately caused the Data Breach and Plaintiff's and members of the Classes' injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Classes, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Classes' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Classes have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

96. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Classes actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Classes)

97. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

98. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Classes' PII.

99. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Classes' sensitive PII.

100. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

101. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Classes.

102. Defendant had a duty to Plaintiff and the members of the Classes to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Classes' PII.

103. Defendant breached its respective duties to Plaintiff and members of the Classes under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Classes' PII.

104. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

105. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Classes, Plaintiff and members of the Classes would not have been injured.

106. The injury and harm suffered by Plaintiff and members of the Classes were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Classes to suffer the foreseeable harms associated with the exposure of their PII.

107. Had Plaintiff and members of the Classes known that Defendant did not adequately protect their PII, Plaintiff and members of the Classes would not have entrusted Defendant with their PII.

108. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Classes have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of Contract
(On Behalf of Plaintiff and the Class)

109. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

110. Defendant entered into various contracts with its clients, including corporations and employers, to provide services to its clients.

111. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential information that Defendant agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

112. Defendant knew that if it were to breach these contracts with its financial provider clients, the clients' consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their PII.

113. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' PII.

114. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

115. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

116. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

117. Plaintiff and members of the Class conferred a benefit upon Defendant in providing PII to Defendant.

118. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's PII, as this was used to facilitate its services to Plaintiff and the Class.

119. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

120. Instead of providing a reasonable level of security, or retention policies, which would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

121. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class's PII because Defendant failed to adequately protect their PII.

122. Plaintiff and Class Members have no adequate remedy at law.

123. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

124. Plaintiff realleges all previous paragraphs as if fully set forth below.

125. Given the relationship between Defendant and Plaintiff and Class Members, where Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

126. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

127. Because of the highly sensitive nature of the PII, Plaintiff and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

128. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII.

129. Defendant also breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

130. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT VI
Invasion of Privacy — Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class)

131. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

132. Plaintiff and the Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

133. Defendant owed a duty to its employees, including Plaintiff and the Class Members, to keep their PII confidential.

134. Defendant failed to protect said PII and exposed the PII of Plaintiff and the Class Members to unauthorized persons which is now publicly available, including on the dark web, and being fraudulently misused.

135. Defendant allowed unauthorized third parties access to and examination of the PII of Plaintiff and the Class Members, by way of Defendant's failure to protect the PII.

136. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class Members is highly offensive to a reasonable person.

137. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class Members PII was disclosed to Defendant as a condition of receiving services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

138. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiff's and the Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

139. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because they had actual knowledge that its information security practices were inadequate and insufficient.

140. Defendant acted with reckless disregard for Plaintiff's and Class Members' privacy when they allowed improper access to its systems containing Plaintiff's and Class Members' PII.

141. Defendant was aware of the potential of a data breach and failed to adequately safeguard their systems and implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' PII.

142. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class Members.

143. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Class Members was disclosed to third parties without authorization, causing Plaintiff and the Class Members to suffer injury and damages as set forth herein, including monetary damages, fraudulent misuse of their PII and fraudulent charges; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and are entitled to compensatory, consequential, and incidental damages as a result of the Data Breach.

144. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class Members.

COUNT VII
Violation of New York Deceptive Trade Practices Act ("GBL")
New York Gen. Bus. Law § 349
(On Behalf of Plaintiff and the Class)

145. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

146. Under the New York Gen. Bus. Law § 349, "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

147. Notably, Defendants' deceptive acts and/or practices were directed at consumers. After all, via its "Privacy Policy" Defendants represented to consumers that they would, *inter alia*, use reasonably adequate data security.

148. And these deceptive acts—including the quotations provided supra—were materially misleading insofar as they induced consumers to rely on such statements and disclose their PII.

149. Section § 349 applies to Defendants because there is a sufficient nexus between Defendants' conduct and New York. After all, Defendant, is headquartered in New York.

150. And, upon information and belief, the misleading acts and/or practices alleged herein—including the manifestations in Defendants' "Privacy Policy"—were written, approved, and/or otherwise authorized by Defendants within the state of New York.

151. In particular, Defendants violated Section § 349 by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

152. Defendants' omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of their PII.

153. Defendants intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

154. Had Defendants disclosed to Plaintiff and Class members that its data systems were not secure—and thus vulnerable to attack—Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants accepted the PII that Plaintiff and Class members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendants' omissions, the truth of which they could not have discovered through reasonable investigation.

155. Defendants acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class members' rights.

156. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

157. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

158. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: July 11, 2024,

Respectfully submitted,

By: /s/ James Bilsborrow
James Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
(212) 558-5500
jbilsborrow@weitzlux.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borrelli (*Pro Hac Vice* forthcoming)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiff and Proposed Class